CLAIMS

What is claimed is:

1. A method for sending a data packet from a first member of a virtual private network to a second member of said virtual private network comprising the steps of:

receiving said data packet enroute to said second member;

determining that said data packet is being sent between members of said virtual private network;

determining the packet manipulation rules for packets sent between members of said virtual private network;

forming a secure data packet by executing said packet manipulation rules on said data packet; and

forwarding said secure data packet to said second member of said virtual private network,

wherein said data packet contains information of a source address and a destination address of said data packet.

2. The method according to claim 1 wherein said step of determining that said data packet is being sent between members of said virtual private network comprises the step of comparing the source and destination addresses of the data packet to addresses stored in a virtual private network address table.

3. The method according to claim 1 wherein said step of determining the packet manipulation rules comprises the step of accessing a lookup table that maintains information identifying compression, encryption and authentication algorithms to be utilized for data packets sent between members of the virtual private network.

4. The method according to claim 3 wherein said step of forming a secure data packet comprises the steps of:

encrypting at least a payload portion of the data packet according to the identified encryption algorithm; and

providing authentication information for the data packet according to the identified authentication algorithm.

5. The method according to claim 3 wherein said forming a secure data packet includes the step of concealing the source and destination addresses of the data packet according to the identified packet manipulation rules.

6. A method for recovering an original data packet from a secure data packet sent between members of a virtual private network comprising the steps of:

receiving said secure data packet;

determining the packet manipulation rules for packets sent between members of said virtual private network;

recovering the original data packet by manipulating the secure data packet by reversing the identified packet manipulation rules; and

forwarding the recovered data packet to its destination,

wherein said source data packet contains information of a source address and a destination address of said secure data packet.

7. The method according to claim 6 wherein said step of determining the packet manipulation rules comprises the step of accessing a lookup table that maintains information identifying compression, encryption and authentication algorithms to be utilized for data packets sent between members of the virtual private network.

8. The method according to claim 7 wherein said recovering step includes the step of recovering the source and destination addresses of the original data packet when they have been concealed.

9. A system for securely exchanging data packets between members of a virtual private network group comprising:

a first computer at a first site, said first computer having a first network address;

a first router associated with said first site for routing data packets originating from said first computer over a public network;

a first virtual private network unit disposed between said first router and said public network, said first virtual ~~public~~ private network unit for identifying virtual private network group data traffic and for securing said data traffic by manipulating said data traffic according to packet manipulation rules maintained by said first virtual private network unit;

a second router associated with a second site for coupling said second site to the public network;

a second virtual private network unit disposed between said second router and the public network for intercepting network traffic destined for said second site, said second virtual ~~public~~ private network unit for detecting virtual private network group traffic and for recovering original packet data; and

a second computer at said second site, said second computer having a second network address for receiving said packet data,

wherein said data packet contains information of a source address and a destination address of said data packet.

10. The system of claim 9 wherein said first and second virtual private network units include means for verifying that

said first and second network addresses are both members of said virtual private network group.

11. The system of claim 10 wherein said first and second virtual private network units each have an associated network addresses, said network traffic utilizing the virtual private network addresses to conceal the identity of the first and second network addresses.